No. 17-2

IN THE

Supreme Court of the United States

UNITED STATES OF AMERICA,

Petitioner,

v.

MICROSOFT CORPORATION,

Respondent.

On Writ of Certiorari to the
United States Court of Appeals for the Second Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND THIRTY-SEVEN TECHNICAL EXPERTS AND LEGAL SCHOLARS IN SUPPORT OF RESPONDENT

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
ELENI KYRIAKIDES
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

January 18, 2018

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF THE *AMICI CURIAE* 1

SUMMARY OF THE ARGUMENT 9

ARGUMENT 10

I. International consensus should establish procedures for law enforcement access to personal data stored in foreign jurisdictions. 12

A. Unilateral law enforcement access by the United States will undermine current efforts to develop procedures for cross-border access to personal data. 13

B. Unilateral law enforcement access triggers conflicts among sovereigns that the presumption against extraterritoriality in U.S. law was intended to avoid. 20

II. Law enforcement access to personal data abroad must comply with international human rights norms. 26

A. Any interference with the fundamental right to privacy must be in pursuit of legitimate aim, in accordance with law, and limited to what is strictly necessary. 27

B. International law mandates numerous safeguards for any regime of electronic surveillance. 31

CONCLUSION 43

TABLE OF AUTHORITIES

CASES

American Banana Co. v. United Fruit Co.,
213 U.S. 347 (1909) 10

EEOC v. Arabian American Oil Co.,
499 U.S. 244 (1991) 20

Kiobel v. Royal Dutch Petroleum Co.,
133 S. Ct. 1659 (2013) 20

Lawrence v. Texas,
539 U.S. 558 (2003) 26

Microsoft v. United States,
829 F.3d 197 (2nd Cir. 2016) 14, 20

Morrison v. National Australia Bank Ltd.,
561 U.S. 247 (2010) 10

Roach v. Elec. Comm'r
(2007) 233 CLR 162 (Austl.) 26

INTERNATIONAL CASES

Ass'n for Eur. Integration and Human Rights v. Bulgaria,
App. No. 62540/00, Eur. Ct. H.R. (2007) 35

C-362/14, *Schrems v. Data Prot. Comm'r*,
2015 E.C.R. 650 ..... 39, 40

C-203/15, *Tele2 Sverige AB v. Post-och telestyrelsen*,
2017 E.C.R. 970 ..... 36, 41

C-293/12, *Digital Rights Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res.*,
2014 E.C.R. 238 ..... 31, 35, 36, 37, 39

Dragojević v. Croatia,
App. No. 68955/11, Eur. Ct. H.R. (2015) 38

Hof van Cassatie [Cass.] [Court of Cassation], Dec. 1, 2015, Pas. 13.2082 N, No. 7, 485 (Belg.) (English translation) 21, 22

Kennedy v. United Kingdom., App. No. 26839/05, Eur. Ct. H.R. (2010) 33

Klass v. Germany, App. No. 5029/71, Eur. Ct. H.R. (1978) 40

Liberty v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. (2008) 11, 34

Puttaswamy v. Union of India, JT 2017 (9) SC 141 ..... 11, 27

Szabó v. Hungary, App. No. 37138/14, Eur. Ct. H.R. (2016) 30, 32

Weber v. Germany, App. No. 54934/00, Eur. Ct. H.R. (2006) 34

Zakharov v. Russia, App. No. 47143/06, Eur. Ct. H.R. (2015) 27, 32, 33, 34, 35, 36, 37, 38, 39, 41

TREATIES & INTERNATIONAL LAW

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, ETS No. 108 18

Council of Europe Convention on Cybercrime, Nov. 23, 2001, S. Treaty No. 108-11 (2003) (ratified Sept. 22, 2006) 15

European Convention on Human Rights, Nov. 4, 1950, ETS No. 005 11

Mutual Legal Assistance Agreement, U.S.-E.U., June 25, 2003, No. 10-201.1 14

Mutual Legal Assistance Treaty, U.S.-Ir., Jan. 18, 2001, T.I.A.S. No. 13137 ..... 11, 14

Regulation 2016/679, 2016 O.J. (L119) 1 (EU) 24

OTHER AUTHORITIES

@JanAlbrecht, Twitter (Jan. 27, 2017, 1:45AM) 25

Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses (2016) 25

Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, Just Security (Sept 16, 2014) 22

Alan McQuinn & Daniel Castro, *How Law Enforcement Should Access Data Across Borders* (2017) 21

Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C 83), 1, 10 (entered into force Dec. 1, 2009) 29, 30, 31

Comm'n Servs., *Improving Cross-border Access to Electronic Evidence: Findings from the Expert Process and Suggested Way Forward* (2017) 17

Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222 ..... 29, 32

Council of Eur., *Chart of Signatures and Ratifications of Treaty 108* (status as of Jan. 11, 2018) 18

Council of Eur., *Details of Treaty 108*, COE.int 18

Cybercrime Convention, Committee, Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime (2017) 15

Eleanor Roosevelt's Legacy: Human Rights, N.Y. Times (Dec. 10, 1988) 28

Elias Groll, *Microsoft vs. the Feds, Cloud Computing Edition*, Foreign Pol'y (Jan. 21, 2016) 21

EPIC, *Council of Europe Privacy Convention* (2018) 18

EPIC, *The Privacy Law Sourcebook: United States Law, International Law and Recent Developments* (Marc Rotenberg ed., 3rd ed. 2016) 2

Eur. Comm'n, *Inception Impact Assessment: Improving cross-border access to electronic evidence in criminal matters* 17

Eur. Comm'n, Inception Impact Assessment (2017) 17

Eur. Comm'n, *Migration and Home Affairs, E-Evidence* (2018) 16

Exec. Order 13768, 82 FR 8799 (Jan. 25, 2017) 25

Francesca Bignami & Giorgio Resta, *Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance* 1 (George Wash. Univ. Law Sch. Pub. Law Research Paper No. 2017-67, 2018) 14

G.A. Res. 217 (III) A, Universal Declaration of Human Rights art. 12 (Dec. 10, 1948) 27

Gianclaudio Malgieri & Paul De Hert, *European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough Oversight, Preferably but not Necessarily by Judges*, 3 Brussels Privacy Hub 1 (2017) 28

Harold Koh, *International Law as Part of Our Law*, 98 Am. J. Int'l L. 43 (2004) 27

Int'l Working Group on Data Prot. in Telecomm., *Common Position on Standards for Data Protection and Personal Privacy in Cross-Border Data Requests for Law Enforcement Purposes* (Final Draft, subject to approval by the Working Group which is foreseen January 22, 2018) 16

International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests: Hearing Before the H. Comm. on the Judiciary, 114th Cong. (2016) 20

International Covenant on Civil and Political Rights, adopted Dec. 16, 1966, S. Exec. Rep. 102–23, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) 28

Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. Nat'l Security L. & Pol'y 473 (2016) 21

Jennifer Daskal, *Rule 41 has been Updated: What's Needed Next*, Just Security (Dec. 5, 2016) 22, 23

Marc Rotenberg, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (EPIC 2nd ed. 2006) 2

Office of Privacy and Civil Liberties, U.S. Dep't of Justice, *Judicial Redress Act of 2015* (2017)..... 25

Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure Before the Jud. Conf. Advisory Comm. on Crim. Rules (2014) (statement of Alan Butler, EPIC Senior Counsel) 23

Ross Anderson, *What Goes Around Comes Around*, in *Privacy in the Modern Age* (Marc Rotenberg, Julia Horwitz, & Jeramie Scott eds., 2015) 26

Statement of the Working Party 29 on the EU-U.S. Umbrella Agreement (Oct. 26, 2016) 25

Supreme People's Court, Supreme People's Procuratorate, Ministry of Public Security, *Handling Certain Issues Concerning the Collection and Examination of Electronic Data in Criminal Cases* (Sept. 20, 2016)..... 23

Susan Hennessey & Chris Mirasola, *Did China Quietly Authorize Law Enforcement to Access Data Anywhere in the World?*, Lawfare (Mar. 27, 2017)..... 23

T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, Fed. Jud. Cent. Int'l Litig. Guide 2014.... 14

The Madrid Privacy Declaration, Nov. 3, 2009 19

The Public Voice, *ENDORSE: Madrid Privacy Declaration – Global Privacy Standards for a Global World*..... 19

U.S. Dep't of State, *Human Rights Reports* (2017) 28

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C.[1] EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

EPIC routinely participates as *amicus curiae* before this Court and other courts in cases concerning privacy issues, new technologies, and constitutional interests. *See, e.g.*, Brief of *Amicus Curiae* EPIC, *Dahda v. United States*, 853 F.3d 1101 (9th Cir. 2017), *cert. granted* 138 S. Ct. 356 (2017) (No. 17-43) (arguing that it is not the Court's role to create "atextual exceptions" to federal privacy laws); Brief of *Amici Curiae* EPIC et. al, *Byrd v. United States*, 679 Fed. App'x 146 (3d Cir. 2017), *cert. granted* 138 S. Ct. 54 (2017) (No. 16-1371) (arguing that modern vehicles store troves of personal data and the status of a driver has no bearing on Fourth Amendment privacy interests); Brief of *Amici Curiae* EPIC et. al, *Carpenter v. United States*, 819 F.3d 880 (6th Cir. 2016), *cert. granted* 137 S. Ct. 2211 (2017) (No. 16-402) (arguing that the Fourth Amendment protects the right against warrantless seizure and search of location data); Brief of *Amicus Curiae* EPIC, *State v. Earls*,

---

[1] Both parties have filed letters of consent to the filing of all amicus briefs with the Clerk of the Court pursuant to Rule 37.3. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

214 N.J. 564 (2013) (same); Brief of *Amici Curiae* EPIC et. al, *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017) (arguing that the First Amendment protects the right to access speech from the privacy of a personal electronic device); Brief of *Amici Curiae* EPIC et. al, *Riley v. California*, 134 S. Ct. 2473 (2014) (arguing that a warrantless search of a cell phone incident to an arrest is impermissible); Brief of *Amicus Curiae* EPIC, *Florida v. Harris*, 586 U.S. 237 (2013) (arguing that the government bears the burden of establishing the reliability of new investigative techniques used in establishing probable cause for a search); Brief of *Amici Curiae* EPIC et. al, *United States v. Jones*, 565 U.S. 400 (2012) (arguing that warrantless tracking of a car using a GPS device violates the Fourth Amendment); Brief of *Amicus Curiae* EPIC, *Commonwealth v. Connolly*, 454 Mass. 808 (2009) (same).

EPIC has a long-standing commitment to international privacy rights. *See, e.g.*, Marc Rotenberg, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (EPIC 2nd ed. 2006); EPIC, *The Privacy Law Sourcebook: United States Law, International Law and Recent Developments* (Marc Rotenberg ed., 3rd ed. 2016) (first edition 1998). In 2010, twenty-nine members of the EPIC Advisory Board wrote to then-Secretary Hillary Clinton, urging U.S. ratification of Council of Europe Convention 108 (the "Privacy Convention"). Letter from Marc Rotenberg, President of EPIC, *et al.* to Secretary of State Hillary Rodham Clinton (Jan. 28, 2010) ("The protection of privacy is a fundamental human right. In the 21st century, it may become one

of the most critical human rights of all.");[2] *see also* EPIC, *Council of Europe Privacy Convention*.[3] EPIC also supported the Madrid Declaration, signed by over one hundred civil society organizations and privacy experts from more than 40 countries, which reaffirms international instruments for privacy protection, identifies new challenges, and calls for concrete actions. *See* Pub. Voice, *Madrid Declaration* (2009).[4]

Most recently, EPIC participated in the development of a Common Position on Standards for data protection and personal privacy in cross-border data requests for law enforcement purposes. Int'l Working Group on Data Prot. in Telecomm., *Common Position on Standards for Data Protection and Personal Privacy in Cross-Border Data Requests for Law Enforcement Purposes* (final draft subject to approval January 22, 2018) (offering recommendations to ensure law enforcement access to cross-border data comport with international human rights norms). EPIC joined the European Digital Rights Initiative (EDRI) in a statement to the Council of Europe recommending revisions to the Budapest Convention on Cybercrime to safeguard human rights. EDRI, *Comments and Suggestions on the Terms of Reference for Drafting a Second Optional Protocol to the Cybercrime Convention* (2017).[5] EPIC participated as *amicus curiae* in *Data Prot. Comm'r v. Facebook*, a case concerning data protection rights in the European

---

[2] https://epic.org/privacy/intl/EPIC_Clinton_ltr_1-10.pdf.

[3] https://epic.org/privacy/intl/coeconvention/.

[4] http://thepublicoice.org/madrid-declaration/.

[5] https://edri.org/files/surveillance/cybercrime_2ndprotocol_globalsubmission_e-evidence_20170908.pdf.

Charter of Fundamental Rights. *Data Prot. Comm'r v. Facebook*, [2017] No. 2016/4809 (Ir.). EPIC has also hosted numerous international conferences exploring global standards for privacy protection. *See, e.g.*, Public Voice, *Emerging Privacy Issues: A Dialogue Between NGOs & DPAs: A Public Voice event, Held in conjunction with the 39th International Conference of Data Protection and Privacy Commissioners* (Sept. 25, 2017).[6]

EPIC seeks to ensure that the U.S. Supreme Court respects the privacy laws of other countries and also does not violate international data protection norms. This case presents a fundamental question about the scope of the Stored Communications Act amid ongoing efforts to develop an international framework for cross-border data transfers.

EPIC submits the following *amicus* brief, signed by distinguished technical experts and legal scholars, in opposition to the exercise of unilateral law enforcement authority that would offend the Court's rule against extraterritorial application of U.S. law and would undermine international norms for data protection.

Technical Experts and Legal Scholars

Alessandro Acquisti
Professor, Carnegie Mellon University

Anita L. Allen
Henry R. Silverman Professor of Law and Philosophy, University of Pennsylvania Law School

---

[6] http://thepublicvoice.org/events/hongkong17/.

Ross Anderson
Professor of Security Engineering, Cambridge University

James Bamford
Author and Journalist

Ann M. Bartow
Director, Franklin Pierce Center for Intellectual Property and Professor of Law, University of New Hampshire School of Law

Colin J. Bennett
Professor, University of Victoria

Francesca Bignami
Professor of Law, George Washington University of Law

Danielle Keats Citron
Morton & Sophia Macht Professor of Law, University of Maryland School of Law

Julie E. Cohen
Mark Claster Mamolen Professor of Law and Technology, Georgetown Law

Simon Davies
Publisher, the Privacy Surgeon, Fellow of the University of Amsterdam, Co-Director of Code Red, Founder of Privacy International and EPIC Senior Fellow

Dr. Whitfield Diffie

David J. Farber
Alfred Fitler Moore Emeritus Professor of Telecommunications, University of Pennsylvania and Adjunct Professor of Internet Studies, Carnegie Mellon University

Addison Fischer
Founder and Chairman, Fischer International Corp.

Hon. David Flaherty
Former Information and Privacy Commissioner for British Columbia

Deborah Hurley
Harvard University and Brown University

Dr. Kristina Irion
Assistant Professor, Institute for Information Law (IViR), University of Amsterdam

Ian Kerr
Canada Research Chair in Ethics, Law & Technology, University of Ottawa Faculty of Law

Chris Larsen
Executive Chairman, Ripple, Inc.

Harry R. Lewis
Gordon McKay Professor of Computer Science, Harvard University

Anna Lysyanskaya
Professor of Computer Science, Brown University

Gary T. Marx
Professor Emeritus of Sociology, MIT

Mary Minow
Library Law Consultant

Dr. Pablo Garcia Molina
Adjunct Professor, Georgetown University

Dr. Peter G. Neumann
Senior Principal Scientist, SRI International Computer Science Lab

Helen Nissenbaum
Professor, Cornell Tech Information Science, Professor, New York University (on leave), Media, Culture, and Communication & Computer Science

Deborah C. Peel, M.D.
President of Patient Privacy Rights

Ronald L. Rivest
Institute Professor of Electrical Engineering and Computer Science, MIT

Pamela Samuelson
Richard M. Sherman Distinguished Professor of Law and Information, University of California, Berkeley School of Law; Co-Director, Berkeley Center for Law & Technology

Bruce Schneier
Fellow and Lecturer, Harvard Kennedy School

Dr. Barbara Simons
IBM Research (retired)

Robert Ellis Smith
Publisher, Privacy Journal

Nadine Strossen
John Marshall Harlan II Professor of Law, New York Law School; Former President, American Civil Liberties Union

Sherry Turkle
Abby Rockefeller Mauzé Professor of the Social Studies of Science and Technology, MIT

Edward G. Viltz
President and Chairman, Internet Collaboration Coalition

Jim Waldo
Gordon McKay Professor of the Practice of Computer Science, Chief Technology Officer, John

A. Paulson School of Engineering and Applied Science, Professor of Technology Policy, Harvard Kennedy School

Christopher Wolf
Board Chair, Future of Privacy Forum

Shoshana Zuboff
Charles Edward Wilson Professor of Business Administration, Emerita, Harvard Business School

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

The Supreme Court faces a blunt choice in this case: whether or not to grant authority for a U.S. law enforcement agency to obtain personal data stored in a foreign jurisdiction. A ruling to allow the search will raise significant sovereignty concerns that the Court's presumption against extraterritorial application of U.S. law was adopted to avoid. A ruling for the government would also invite other countries to disregard sovereign authority. And a ruling for the government would undermine efforts to develop new procedures, based on international consensus, for cross border data access. But a ruling that respects the authority of foreign sovereigns will avoid a cascade of international conflict.

In addition, the Supreme Court should not authorize searches in foreign jurisdictions that violate international human rights norms. The European Convention on Human Rights and the EU Charter of Fundamental Rights make clear that privacy is a fundamental right. Where there is an interference with the right to privacy, it must be in accordance with law, for a legitimate purpose, and limited to what is necessary in a democratic society. The European Court of Human Rights and the European Court of Justice have issued many foundational opinions that safeguard the right to privacy in the digital age. The U.S. Supreme Court should not act in contravention of other high courts in matters of fundamental rights.

ARGUMENT

For over a century, this Court has emphasized that "it is a longstanding principle of American law 'that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.'" *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247, 248 (2010). At the outset, this Court recognized:

> the general and almost universal rule is that the character of an act as lawful or unlawful must be determined wholly by the law of the country where the act is done. For another jurisdiction, if it should happen to lay hold of the actor to treat him according to its own notions rather than those of the place where he did the acts, not only would be unjust, but would be an interference with the authority of another sovereign, contrary to the comity of nations, which the other state concerned justly might resent . . .

American Banana Co. v. United Fruit Co., 213 U.S. 347 (1909) (internal citations omitted). The search in this case raises precisely the type of sovereignty and comity concerns that underlie the Court's presumption against extraterritorial application of U.S. law.

There is already a clear and present risk that the unilateral exercise of extraterritorial jurisdiction to search personal data will cause international conflicts. Other nations seek access to personal data beyond their national borders. A holding that U.S. law enforcement agents may compel private companies to disclose private communications stored in another

national jurisdiction invites a global "free-for-all." Any country could seek data stored anywhere in the world, including in the United States, based only on that nation's judicial authority. This Court should not encourage that outcome.

There are in place well established procedures to permit access to personal data stored outside a nation's jurisdiction. *See* Mutual Legal Assistance Treaty, U.S.-Ir., Jan. 18, 2001, T.I.A.S. No. 13137. And the international community is developing additional procedures to address emerging issues. The Council of Europe, the International Working Group on Data Protection in Telecommunications, and the European Commission are each developing frameworks for trans-border access to electronic evidence. A grant of unilateral authority to U.S. law enforcement agencies in this case will undermine current treaty obligations and disrupt joint efforts to address new challenges.

But regardless of the extraterritorial effects of this Court's decision, the U.S. Supreme Court should not authorize access to data in foreign jurisdictions where such access violates international human rights norms. According to well-established principles of international law, any interference with the right to privacy must be in accordance with law, for a legitimate purpose, and limited to what is necessary in a democratic society. European Convention on Human Rights art. 8, Nov. 4, 1950, ETS No. 005; *Liberty v. United Kingdom*, App. No. 58243/00, Eur. Ct. H.R., Judgment, 26 (2008);[7] *Puttaswamy v. Union of India*, JT 2017 (9) SC 141 (discussing European Court of Human Rights & European Court of Justice prece-

[7] http://hudoc.echr.coe.int/eng?i=001-87207.

dent in holding privacy is a fundamental right under the Indian Constitution).[8]

The decision in this case will have an international impact. Other courts will look to this Court to determine how best to address electronic searches in jurisdictions outside their borders. The Court should therefore take special heed of international data protection standards.

I. International consensus should establish procedures for law enforcement access to personal data stored in foreign jurisdictions.

International tensions police access to personal data loom large in the background of this case.[9] Many governments have already asserted authority to obtain personal data stored outside their borders. The problem is well understood, which is the reason that international organizations are now developing international frameworks for law enforcement access that respect data protection standards. A decision to

---

[8] http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

[9] *See, e.g.*, Brief of Former Law Enforcement, National Security, and Intelligence Officials as Amicus Curiae Supporting Neither Party at 18, *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016), *cert. granted sub nom. United States v. Microsoft Corp.*, No. 17-2, 2017 WL 2869958 (U.S. Dec. 13, 2017) (citing potential "collateral effects" of the court's decision, including "decreased international cooperation in law enforcement"). Rarely is there agreement between civil liberties organizations and former law enforcement officials as to the risks of a particular outcome in a matter before this Court.

allow courts in the United States to compel disclosure of personal data stored abroad would interfere with ongoing efforts to resolve this dispute.

In contrast, a ruling that respects the presumption against the extraterritorial enforcement of a domestic law would provide the breathing room necessary for the development of international frameworks. Multinational bodies—including the Council of Europe, the International Working Group on Data Protection in Telecommunications, and the European Commission—are currently developing proposals to address cross-border data protection and law enforcement cooperation standards. The international community is better positioned than any one country to consider and respond to the wide range of interests at stake. Similar negotiations have previously led to historic international agreements around privacy, including Council of Europe Convention 108 (The "Privacy Convention") and the Madrid Declaration of 2009.

A. Unilateral law enforcement access by the United States will undermine current efforts to develop procedures for cross-border access to personal data.

Limiting the reach of the Stored Communications Act to the United States would not only conform with the presumption against extraterritoriality, it would also avoid a cascade of international conflict and facilitate the development of data protection and cross-border access standards through international consensus. *See, e.g.*, Francesca Bignami & Giorgio Resta, *Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance* 1 (George Wash. Univ. Law Sch. Pub. Law Research Paper No.

2017-67, 2018) ("[T]he old international system of states and territory cannot serve as an ordering device for the borderless Internet, and the social interactions fostered by borderless digital communications should give rise to a common set of moral commitments . . . .").[10]

A customary mechanism for international cooperation on cross-border access by law enforcement agencies is available to the U.S. in this case: a Mutual Legal Assistance Treaty (MLAT). "The MLAT is a treaty-based mechanism for seeking foreign law enforcement cooperation and assistance in support of an ongoing criminal investigation or proceeding," which includes U.S. court and executive oversight. T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, Fed. Jud. Cent. Int'l Litig. Guide 2014, at 4. The U.S. has negotiated an MLAT with Ireland. *See* Mutual Legal Assistance Treaty, U.S.-Ir., Jan. 18, 2001, T.I.A.S. No. 13137. This bilateral agreement is supplemented by an MLAT between the U.S. and EU. *See* Mutual Legal Assistance Agreement, U.S.-E.U., June 25, 2003, No. 10-201.1. These treaties recognize of the need for cooperation in a sensitive area of cross-border data access. *See Microsoft v. United States*, 829 F.3d 197, 221 (2016) (stating "the MLAT process reflects" the interests of comity). Indeed, the preamble to the U.S.-EU MLAT includes the phrases: "DESIRING further to facilitate cooperation," and "HAVING DUE REGARD for rights of individuals and the rule of law." *Id.* at 4 (emphasis in original).

---

[10] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043771.

However, as new challenges have arisen, the international community is updating standards and agreements for data protection and cross-border access. For example, the Council of Europe is now considering proposals to update the 2001 Council of Europe Convention on Cybercrime ["Cybercrime Convention"], Nov. 23, 2001, S. Treaty No. 108-11 (2003) (ratified Sept. 22, 2006), which the U.S. signed in 2001 and ratified in 2006. This Convention previously addressed cross-border data transfers. Article 32 of the Cybercrime Convention provides for "[t]ransborder access to stored computer data with consent or when publicly available." Convention on Cybercrime, Nov. 23, 2001, S. Treaty No. 108-11 (2003) (ratified Sept. 22, 2006).[11] In June 2017, the Committee established the terms of reference for developing a 2nd Additional Protocol to the Cybercrime Convention to enhance international cooperation on the issue. Cybercrime Convention, Committee, Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, 17th Sess., Doc. No. 3 (2017).[12] The Committee anticipates that the Additional Protocol will be finalized by December 2019 and will include provisions on "more effective mutual legal assistance" and "direct cooperation with service providers in other jurisdictions." *Id.* The Committee has also called for a "clearer frame-

---

[11] http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

[12] https://rm.coe.int/terms-of-reference-for-the-preparation-ofa-draft-2nd-additional-proto/168072362b.

work and stronger safeguards for existing practices of transborder access to data." *Id.*

The International Working Group on Data Protection in Telecommunications ["IWG"] has also recently drafted a Common Position on cross-border law enforcement requests. Int'l Working Group on Data Prot. in Telecomm., *Common Position on Standards for Data Protection and Personal Privacy in Cross-Border Data Requests for Law Enforcement Purposes* (final draft subject to approval January 22, 2018). The IWG Common Position ensures that cross-border law enforcement data requests accord with international human rights norms and afford appropriate data protection safeguards. *Id.* The Common Position includes, in part, recommendations for notice when no longer likely to jeopardize the investigation, judicial authorization, oversight of the cross-border data regime, and transparency mechanisms (i.e. aggregate statistical reporting). *Id.*

Other countries will soon begin the process of adopting multinational standards for cross-border access to evidence. For example, the European Commission will propose legislation to address this issue in early 2018. Eur. Comm'n, *Migration and Home Affairs, E-Evidence* (last updated Jan. 4, 2018).[13] This legislation is intended to "[i]mprove cross-border access to electronic evidence in criminal matters." Eur. Comm'n, *Inception Impact Assessment: Improving*

---

[13] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en.

cross-border access to electronic evidence in criminal matters.[14]

This legislation reflects the process of policy development, assessment, and consultation within the European Union. For instance, in 2017 the Commission proposed a plan for "improving cross-border access to electronic evidence." Comm'n Servs., *Improving Cross-border Access to Electronic Evidence: Findings from the Expert Process and Suggested Way Forward* (2017).[15] The proposal included "practical measures" (specific suggestions to improve cooperation via training, an efficient online platform to create request, and increased dialogue) and "legislative solutions" (including proposing EU wide cross-border production requests, international agreements, and direct access) to address the complicated range of issues presented by cross-border data access. Eur. Comm'n, *Inception Impact Assessment* (2017).[16] As part of this process, the European Commission consulted with experts, Member States, NGOs, and the public on the range of policy options. *Id.*

Past examples have shown that international privacy agreements provide the best opportunity to establish data protection standards for cross-border access to personal data. For example, in 1981 the Council of Europe established Convention 108 (also

---

[14] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en.

[15] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf.

[16] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en.

referred to as the "International Privacy Convention)" to strengthen the legal protection of individuals with regard to automatic processing of personal information. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, ETS No. 108.[17] The Convention:

> Provid[es] guarantees in relation to the collection and processing of personal data, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards... and enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected.

Council of Eur., *Details of Treaty 108*, COE.int.[18] The Privacy Convention is the first binding international legal instrument on data protection, and is open to any country, including non-members of the Council of Europe. *Id.*; *see also* EPIC, *Council of Europe Privacy Convention* (2018).[19] A total of 51 countries, including all of the members of the Council of Europe and eight non-members, have ratified the International Privacy Convention. Council of Eur., *Chart of Signatures and Ratifications of Treaty 108* (status as of Jan. 11, 2018).[20] A coalition of civil society organiza-

---

[17] https://rm.coe.int/1680078b37.

[18] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

[19] https://epic.org/privacy/intl/coeconvention/.

[20] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures.

tions campaigned for national governments, including the United States, to ratify the Council of Europe Privacy Convention and to adopt comprehensive privacy legislation based on the Convention. EPIC, *Council of Europe Privacy Convention* (2018).[21]

Over 100 civil society organizations and privacy experts from more than 40 countries also set out the Madrid Privacy Declaration, which also established international norms for data protection. *See* The Madrid Privacy Declaration, Nov. 3, 2009;[22] The Public Voice, *ENDORSE: Madrid Privacy Declaration – Global Privacy Standards for a Global World.*[23] The Madrid Declaration affirms that privacy is a fundamental right and sets out ten statements from civil society. Critically, the Madrid Declaration urges countries "that have not yet established a comprehensive framework for privacy protection and an independent data protection authority to do so as expeditiously as possible" and calls for the "establishment of a new international framework for privacy protection, with the full participation of civil society, that is based on the rule of law, respect for fundamental human rights, and support for democratic institutions." *Id.*

The international community is already hard at work developing data protection standards for cross border access to personal data. Prior efforts to create international frameworks governing interna-

---

[21] https://epic.org/privacy/intl/coeconvention/.

[22] http://thepublicvoice.org/TheMadridPrivacy Declaration.pdf.

[23] http://thepublicvoice.org/madrid-declaration/endorsement/.

tional privacy issues have been successful. However, unilateral law enforcement access to personal data in foreign jurisdictions will create conflicts among sovereigns and international cooperation.

B. Unilateral law enforcement access triggers conflicts among sovereigns that the presumption against extraterritoriality in U.S. law was intended to avoid.

Courts are not well suited to make policy decisions in the "delicate field of international relations." *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659 (2013). That is why the Court has consistently applied a presumption against extraterritorial enforcement of U.S. law, to protect against "unintended clashes between our laws and those of other nations which could result in international discord." *EEOC v. Arabian American Oil Co.*, 499 U.S. 244, 248 (1991). In the privacy and data protection context, clashes occur whenever a country asserts a unilateral right to access data stored in a foreign jurisdiction. As the lower court noted, a decision to limit the reach of the SCA "serves the interests of comity" which "ordinarily govern the conduct of cross boundary criminal investigations." *Microsoft v. United States*, 829 F.3d 197, 221 (2d Cir. 2016).

The decisions of national courts to approve police access to data outside their jurisdictions has already caused international conflict. *See International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. (2016) (discussing law enforcement data transfers with Ireland, the U.K., and more); *see also* Jennifer Daskal, *Law*

Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues, 8 J. Nat'l Security L. & Pol'y 473 (2016).[24] The protections Congress established in the Stored Communications Act, in particular, would be undermined by such unilateral access.

For example, in 2015, Brazilian authorities ordered Microsoft to hand over Skype user data stored inside the United States in connection with an investigation under way in Brazil. *See* Alan McQuinn & Daniel Castro, *How Law Enforcement Should Access Data Across Borders* 9 (2017).[25] Microsoft refused, contending disclosure of the data would violate the privacy protections guaranteed Americans under the U.S. Electronic Communications Privacy Act. Elias Groll, *Microsoft vs. the Feds, Cloud Computing Edition*, Foreign Pol'y (Jan. 21, 2016).[26] Brazilian authorities proceeded to arrest a Microsoft executive. *Id.*

The same year, the Supreme Court in Belgium confirmed a judgment of the Court of Appeal of Antwerp (the "Court of Appeal") and imposed a significant fine on Yahoo! for failing to produce IP addresses for a domestic investigation. *Hof van Cassatie* [Cass.] [Court of Cassation], Dec. 1, 2015, Pas. 13.2082 N, No. 7, 485 (Belg.) (English translation).[27]

---

[24] http://jnslp.com/wp-content/uploads/2016/11/Law_Enforcement_Access_to_Data_Across_Borders_2.pdf.

[25] http://www2.itif.org/2017-law-enforcement-data-borders.pdf.

[26] http://foreignpolicy.com/2016/01/21/microsoft-vs-the-feds-cloud-computing-edition/.

[27] http://journals.sas.ac.uk/deeslr/article/viewFile/2310/2261.

Yahoo! argued that Belgium's actions violated the UN Charter and customary international law, which provides that a "State may in principle not perform any executive jurisdiction outside its territory." *Id.* at 1. Accordingly, the company argued that Belgium "fails to recognize the principal of sovereign equality of States." *Id.* The Court found Yahoo! was territorially present in Belgium through its active participation in Belgian economy and therefore voluntarily submits itself to Belgian authority and jurisdiction. *Id.* at 9. Under such a standard, Belgium could assert unilateral authority to access data in the United States without regard to the SCA or any other privacy laws.

The increasing use of remote access search techniques by law enforcement will likely accelerate international conflict. Hacking by law enforcement typically entails "remote access of a computer to install malicious software" over the internet. Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, Just Security (Sept 16, 2014).[28] After the software is installed, the "malware controls the target computer." *Id.* The Court recently approved certain changes to Rule 41 related to remote access searches. *See* Jennifer Daskal, *Rule 41 has been Updated: What's Needed Next*, Just Security (Dec. 5, 2016).[29] During proceedings before the rules committee that proposed the changes, the U.S. Department of Justice conceded

---

[28] https://www.justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance/.
[29] https://www.justsecurity.org/35136/rule-41-updated-needed/.

that "in at least some situations the government will be remotely searching data or a device that is located extraterritorially." *Id.* In addition to the problems posed by the extraterritoriality of remote searches, the changes also did not adequately provide for notice to the targets of the search as required by law. *See Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure Before the Jud. Conf. Advisory Comm. on Crim. Rules* (2014) (statement of Alan Butler, EPIC Senior Counsel).[30]

Other countries are deploying techniques for extraterritorial access to personal data. Chinese regulations permit remote "extraction," or copying, of data located outside its borders. Supreme People's Procuratorate, Ministry of Public Security, *Handling Certain Issues Concerning the Collection and Examination of Electronic Data in Criminal Cases* (Sept. 20, 2016).[31] The Chinese regulations state data may be extracted online through the network. *Id.* at art. 9. Though the extent of this authority is unclear in practice, commenters have warned that "Chinese officials have authorization to remotely search or extract data anywhere in the world, subject only to the limitations of domestic law." Susan Hennessey & Chris Mirasola, *Did China Quietly Authorize Law Enforcement to Access Data Anywhere in the World?*, Lawfare (Mar. 27, 2017).[32]

---

[30] https://epic.org/privacy/surveillance/remote-access/EPIC-FRCP-Rule-41-Amendments-Testimony.pdf.

[31] http://www.spp.gov.cn/xwfbh/wsfbt/201609/t20160920_167380_1.shtml.

[32] https://www.lawfareblog.com/did-china-quietly-authorize-law-enforcement-access-data-anywhere-world.

Any unilateral foreign access to data stored in Ireland may also contravene EU law and U.S. international commitments. The EU General Data Protection Regulation (GDPR), will take effect on May 25, 2018. Regulation 2016/679, 2016 O.J. (L119) 1 (EU). This law will bind Ireland, where the data at issue in this case is stored. Article 48 of the GDPR provides:

> Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

GDPR art. 48. The GDPR thus restricts data transfers without an adequate basis under EU law. The GDPR also makes clear that only MLATs, or similar international agreements, provide a permissible basis for the extraterritorial transfer of personal data.

The recently adopted Data Protection and Privacy Agreement (DPPA), also described as "the Umbrella Agreement," governs law enforcement data transfers between the EU and the U.S. *See* Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, De-

tection, and Prosecution of Criminal Offenses (2016).[33] The DPPA "establishes a set of protections that the Parties are to apply to personal information exchanged for the purpose of preventing, detecting, investigating, or prosecuting criminal offenses." Office of Privacy and Civil Liberties, U.S. Dep't of Justice, *Judicial Redress Act of 2015* (2017).[34]

Article 19 of the agreement establishes "an obligation for the Parties to provide, in their domestic law, specific judicial redress rights to each other's citizens." Statement of the Working Party 29 on the EU-U.S. Umbrella Agreement (Oct. 26, 2016).[35]The Judicial Redress Act, 5 U.S.C. § 552a note implements Article 19, providing it with the force of law. Indeed, when a recent Executive Order limited Privacy Act protections for foreigners, permitting the use of personal data outside the scope of the Act, Exec. Order 13768, 82 FR 8799 (Jan. 25, 2017), members of the European Parliament quickly threatened sanctions, contending that the U.S. may have broken the Agreement. *See, e.g.*, @JanAlbrecht, Twitter (Jan. 27, 2017, 1:45AM).[36]

If more countries assert unilateral authority to access data outside of their national borders (through judicial order, remote access, or otherwise) it will

---

[33] https://www.justice.gov/opcl/DPPA/download.

[34] https://www.justice.gov/opcl/judicial-redress-act-2015.

[35] http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20161026_statement_of_the_wp29_on_the_eu_umbrella_agreement_en.pdf.

[36] https://twitter.com/JanAlbrecht/status/824553962678390784.

cause substantial conflict and interfere with ongoing trade and cooperation agreements. The United States' assertion of such unilateral authority could accelerate this trend. The Court should heed its well-established rule against the extraterritorial application of U.S. law.

II. Law enforcement access to personal data abroad must comply with international human rights norms.

The U.S. law enforcement demand for personal data stored in Ireland necessarily implicates the decisions and authority of the European Court of Human Rights and the European Court of Justice. These courts have established fundamental principles that govern privacy and data protection. Because of the international dimensions of this case, the Court should be careful not to conflict with international norms for the protection of privacy. *See* Ross Anderson, *What Goes Around Comes Around*, in *Privacy in the Modern Age* (Marc Rotenberg, Julia Horwitz, & Jeramie Scott eds., 2015). Regardless of how the Court assesses the extraterritorial application of U.S. law, the Court should ensure that law enforcement cross-border data requests comport with international human rights norms. The European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights (the "Charter") recognize a fundamental right to privacy and carry substantial authority with high courts around the world. *See, e.g.*, *Lawrence v. Texas*, 539 U.S. 558, 576 (2003) (citing European Court of Human Rights cases regarding Article 8 of the European Convention); *Roach v. Elec. Comm'r* (2007) 233 CLR 162, 179–83, 203–4 (Austl.) (same). *Puttaswamy*, JT 2017 (9) SC 141 (discussing

European Court of Human Rights & European Court of Justice precedent in holding privacy is a fundamental right under the Indian Constitution). *See also* Harold Koh, *International Law as Part of Our Law*, 98 Am. J. Int'l L. 43, 45 (2004) ("From the beginning, then, American courts regularly took judicial notice of both international law and foreign law," to ignore them "would constitute a stunning reversal of history.").

International norms mandate that an interference with the right to privacy must be in accordance with law, for a legitimate purpose, and limited to what is necessary in a democratic society. Foundational opinions from the European Court of Human Rights (ECtHR) and European Court of Justice (ECJ) have established numerous safeguards for government monitoring of electronic communications. *Zakharov v. Russia*, App. No. 47143/06, Eur. Ct. H.R., Judgment, 60 (2015).[37]

A. Any interference with the fundamental right to privacy must be in pursuit of legitimate aim, in accordance with law, and limited to what is strictly necessary.

Numerous international instruments recognize privacy as a fundamental human right—a right implicated by the disclosure of personal data at issue in this case. *See, e.g.*, G.A. Res. 217 (III) A, Universal Declaration of Human Rights art. 12 (Dec. 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor

---

[37] http://hudoc.echr.coe.int/eng?i=001-159324

to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."); International Covenant on Civil and Political Rights, art. 17, adopted Dec. 16, 1966, S. Exec. Rep. 102–23, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976). The United States has long helped establish and maintain international norms for privacy protection. *See, e.g.*, *Eleanor Roosevelt's Legacy: Human Rights*, N.Y. Times (Dec. 10, 1988) (describing Eleanor Roosevelt's role in shaping UDHR as chairman of U.N. Commission on Human Rights);[38] U.S. Dep't of State, *Human Rights Reports* (2017) (annual "Country Reports on Human Rights Practices" assessing practices against UDHR and other instruments).[39]

Among international instruments, the European Convention on Human Rights (the "European Convention") and the Charter of Fundamental Rights for the European Union (the "European Charter") are enormously influential. *See, e.g.*, Gianclaudio Malgieri & Paul De Hert, *European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough Oversight, Preferably but not Necessarily by Judges*, 3 Brussels Privacy Hub 1, 1 (2017). Article 8 of the European Convention states:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.

---

[38] http://www.nytimes.com/1988/12/10/opinion/eleanor-roosevelt-s-legacy-human-rights.html.

[39] https://www.state.gov/j/drl/rls/hrrpt/.

> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter "European Convention"].

Articles 7 and 8 of the European Charter set out fundamental rights for all natural persons in the European Union. Article 7 on the "Respect for private and family life" states:

> Everyone has the right to respect for his or her private and family life, home and communications.

Charter of Fundamental Rights of the European Union, art. 7, Dec. 18, 2000, 2000 O.J. (C 83), 1, 10 (entered into force Dec. 1, 2009) [hereinafter "European Charter"]. Article 8 on the "Protection of personal data" states:

> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by

> law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

Charter art. 8.

The European Court of Human Rights, applying the European Convention, and the European Court of Justice, applying the European Charter, have established a common jurisprudence for privacy protection. The European Court of Human Rights will evaluate whether there has been an interference with privacy rights under Article 8 of the European Convention, and, if so, whether that interference is necessary to pursue a "legitimate aim[]," is "in accordance with law" and "is necessary in a democratic society in order to achieve any such aim." *Szabó v. Hungary*, App. No. 37138/14, Eur. Ct. H.R., Judgment, 33 (2016).[40] Likewise, if the European Court of Justice identifies an interference with the rights under Articles 7 and 8 of the European Charter, that interference must be justified under the test found in Article 52(1):

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be

[40] http://hudoc.echr.coe.int/eng?i=001-160020.

> made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Charter art. 52(1). *See e.g.*, C-293/12, *Digital Rights Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res.*, 2014 E.C.R. 238, ¶¶ 38–69 (applying this test in the context of an interference with Articles 7 and 8). Where data privacy rights are concerned, the Court of Human Rights and Court of Justice both require that an interference to meet a heightened "strict necessity" standard. *Szabó*, App. No. 37138/14, Eur. Ct. H.R., at 33; *Digital Rights Ir. Ltd.*, 2014 E.C.R. at ¶ 52.

B. International law mandates numerous safeguards for any regime of electronic surveillance.

Applying the multi-pronged test to assess the validity of an interference with the right to privacy, the European Court of Human Rights and, recently, the European Court of Justice,[41] have established minimum standards to restrict government electronic surveillance.[42] These standards take into account the

---

[41] The European Charter, including its privacy guarantees, became legally binding in 2009 with the Treaty of Lisbon's entry into force. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) 1 171 (entered into force Dec. 1, 2009).

[42] The terms communications or electronic "surveillance" are used throughout this brief to refer to government ac-

nature of the offenses for which an order can be issued and the categories of individuals who may be affected. *See, e.g.*, *Szabó*, App. No. 37138/14, Eur. Ct. H.R., at 30–44 (analysis therein). Courts have indicated a preference for prior judicial review and a sufficient factual basis for any surveillance of an individual. *Id.* The standards also require independent post-authorization oversight. *Id.* Courts also require a number of other safeguards under the categorical analysis.

The European Court of Human Rights established these safeguards, following careful review of the statutes' lawfulness and necessity. *Id.* at 34; *Zakharov*, App. No. 47143/06, Eur. Ct. H.R., at 59. Where, as here, authorities request access to personal data for serious criminal law enforcement purposes, there is still an interference with Article 8 Rights under the European Convention. *See, e.g.*, *Szabó*, App. No. 37138/14, Eur. Ct. H.R., at 32 ("[T]he mere existence of the legislation . . . constitutes an interference by a public authority . . . ."); ECHR art. 8 § 2 (recognizing the interests of "national security, public safety . . . for the prevention of disorder or crime"). The central assessment for the legitimacy of a surveillance regime is therefore whether it is in accordance with law and strictly necessary.

Under the European Convention, the legality and necessity of a surveillance regime is assessed based on each following categorical safeguards:

> the accessibility of the domestic law, the

---

cess to communications information, including personal data.

> scope and duration of the secret surveillance measures, the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data, the authorisation procedures, the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law.

Zakharov, App. No. 47143/06, Eur. Ct. H.R., at 60.

(1) Accessibility

The terms of surveillance must be "accessible" or publicly available. *Zakharov v. Russia*, App. No. 47143/06, Eur. Ct. H.R., at 60. *See also Kennedy v. United Kingdom.*, App. No. 26839/05, Eur. Ct. H.R., Judgment, 38 (2010) (analyzing that there was no dispute the surveillance at issue had a basis in domestic law which was publicly available).[43] For example, in *Zakharov*, the European Court of Human Rights noted the Russian government's failure to publish addendums to a technical document on interception equipment that was "capable of affecting the users' right to respect for their private life and correspondence." *Zakharov*, App. No. 47143/06, Eur. Ct. H.R., at 60–61. Similarly, in *Liberty v. United Kingdom*, annual reports in which the UK Secretary of State's would merely affirm, without further detail, that "arrangements" followed to ensure restricted access to material collected via surveillance "did not contribute towards the accessibility and clarity of the

---

[43] http://hudoc.echr.coe.int/eng?i=001-98473.

scheme, since he was not able to reveal what the 'arrangements' were." App. No. 58243/00, Eur. Ct. H.R., Judgment, 26 (2008).[44]

(2) Foreseeability/scope of application

The terms of surveillance must also be reasonably foreseeable. The scope of any authorization must be defined with enough precision to give "an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures." *Zakharov*, App. No. 47143/06, Eur. Ct. H.R., at 61. This includes clearly defining both the "nature of the offences which may give rise" to an order and "a definition of the categories of people liable to" to be surveilled. *Id.* For instance, the Court of Human Rights found that Russian law was not reasonably foreseeable. *Id.* at 62 Under the statute, surveillance could be ordered for "a person who may have information about a criminal offence" or "have information relevant to the criminal case," but legislation and court precedent did not define those terms. *Id.*. In contrast, the European Court of Human Rights held in *Weber v. Germany* that a German surveillance law was reasonably foreseeable. App. No. 54934/00, Eur. Ct. H.R., Decision as to Admissibility, 23 (2006).[45] The exact offenses for which surveillance could be ordered were provided in the statute. *Id.* The law also required that the target must have made an international phone call using specific technologies or saying specific catchwords, or the target must be within a category of foreigners or companies whose lines could be monitored deliberately. *Id.*

---

[44] http://hudoc.echr.coe.int/eng?i=001-87207.

[45] http://hudoc.echr.coe.int/eng?i=001-76586.

(3) Duration of the secret surveillance measures

The duration of any surveillance must also be appropriately restricted. A determination over duration may be left to "relevant domestic authorities which have competence to issue and renew interception warrants," but only if there are sufficient safeguards in place. *Zakharov*, App. No. 47143/06, Eur. Ct. H.R., at 63. Appropriate restrictions on duration include a "clear indication in the domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled." *Id.* In *Ass'n for Eur. Integration and Human Rights v. Bulgaria*, for example, the European Court of Human Rights found surveillance appropriately circumscribed at least at the "initial stages" where it could be "authorised for a maximum of two months" and "may be extended, up to six months, only pursuant to a fresh application and warrant." App. No. 62540/00, Eur. Ct. H.R., Judgment, 19 (2007).[46]

On the other hand, in *Digital Rights Ireland*, the European Court of Justice invalidated the Data Retention Directive that required retention of communications data for at least six and up to twenty-four months without any objective criteria to either limit the data initially retained or to determine which data should be stored for more than the six month minimum. C-293/12, *Digital Rights Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res.*, 2014 E.C.R. 238, ¶¶ 63–64. The European Court concluded the Directive "entails a wide-ranging and particularly se-

---

[46] http://hudoc.echr.coe.int/eng?i=001-81323.

rious interference... without... being precisely circumscribed." *Id.* at ¶ 65.

(4) Storing, accessing, examining, using, communicating and destroying intercepted data.

A surveillance regime must also be cabined by "procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data." *Zakharov*, App. No. 47143/06, Eur. Ct. H.R., at 63. *See also* C-203/15, *Tele2 Sverige AB v. Post-och telestyrelsen*, 2017 E.C.R. 970, ¶¶ 116–17 (stating legislation must "lay down clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data"). For example, in *Zhakarov*, the Court of Human Rights concluded that "Russian law contains clear rules governing the storage, use and communication of intercepted data, making it possible to minimise the risk of unauthorised access or disclosure," such as secure storage and access only with security clearances. App. No. 47143/06, Eur. Ct. H.R., at 63–64. However, the court faulted the Russian law for both the "lack of a requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained" and permitting "unlimited discretion to the trial judge to store or to destroy the data used in evidence after the end of the trial." *Id.* at 64.

(5) Authorization procedures

According to the European Court of Human Rights, any procedures authorizing surveillance must ensure that it is "not ordered haphazardly, irregularly or without due and proper consideration." *Zakharov*, App. No. 47143/06, Eur. Ct. H.R., at 64–65. First,

any authorization should, preferably, be subject to rigorous prior judicial review. Second, any surveillance should be ordered only after authorities provide an individualized factual basis for surveilling the target.

First, authorization should, preferably, be subject to prior judicial review. A "non-judicial authority" is permissible only provided that that authority is "sufficiently independent from the executive." *Zakharov*, App. No. 47143/06, Eur. Ct. H.R., at 65. "Control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny." *Szabó*, App. No. 37138/14, Eur. Ct. H.R., at 40. The European Court of Human Rights has explained:

> the rule of law implies . . . that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.

Id. See also C-293/12, *Digital Rights Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res.*, 2014 E.C.R. 238, ¶ 62. (disfavoring "access by the competent national authorities to the data retained [that] is not made dependent on a prior review carried out by a

court or by an independent administrative body."). Further, any provision for an emergency authorization without judicial review should be strictly limited and subject to "post factum review," *Szabó*, App. No. 37138/14, Eur. Ct. H.R., at 42.

Second, any authorization procedures must ensure "sufficient reasons for intercepting a specific individual's communications exist in each case." *Zakharov*, App. No. 47143/06, Eur. Ct. H.R., at 62. The reviewing authority must be provided sufficient information to:

> be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security . . .

Id. at 65. In *Dragojević v. Croatia*, for instance, the European Court of Human Rights found a violation of Article 8 rights where surveillance was ordered without the provision of "details . . . based on the specific facts of the case and particular circumstances indicating a probable cause to believe that the offences had been committed and that the investigation could not be conducted by other, less intrusive, means." App. No. 68955/11, Eur. Ct. H.R., Judgment, 27 (2015).[47] Similarly in *Schrems v Data Prot. Comm'r*, the European Court of Justice found that legislation

---

[47] http://hudoc.echr.coe.int/eng?i=001-150298.

may not authorize "on a generalised basis" storage and access to "all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued." C-362/14, *Schrems v. Data Prot. Comm'r*, 2015 E.C.R. 650, ¶ 93. *See also* C-293/12, *Digital Rights Ir. Ltd. v. Minister for Commc'ns, Marine & Nat. Res.*, 2014 E.C.R. 238, ¶¶ 57-29 (condemning a data retention directive's "appli[cation] even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.").

(6) Supervision

Post-authorization supervision has also been emphasized as essential safeguard in any surveillance regime. As the European Court of Human Rights has explained, "supervision arrangements" should be "capable of ensuring that the statutory requirements relating to the implementation of the surveillance measures, the storage, access to, use, processing, communication and destruction of intercept material are routinely respected" after-the-fact of the initial surveillance. *Zakharov*, App. No. 47143/06, Eur. Ct. H.R., at 69–70. In *Klass v. Germany*, for instance, the European Court of Human Rights approved supervision by two German bodies which had demonstrable independence, powers, and competence, and, in particular, where one body had "democratic character" evident in the representation from the opposition party in its member-

ship. App. No. 5029/71, Eur. Ct. H.R., Judgment, 21 (1978).[48] In *Schrems v. Data Prot. Comm'r*, the European Court of Justice recognized a critical role of data protection authorities as a supervisory mechanism, concluding: "national supervisory authorities must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him." C-362/14, *Schrems v. Data Prot. Comm'r*, 2015 E.C.R. 650, ¶ 99.

On the other hand, the European Court of Human Rights deemed a bi-annual private report to parliamentary committee on the functioning of national security services insufficient to "redress to any individual grievances caused by secret surveillance" or to meaningfully control "the daily functioning of the surveillance organs." *Szabó*, App. No. 37138/14, Eur. Ct. H.R., at 42.

(7) Notice and remedies

Finally, according to the European Court of Human Rights, notice and an effective remedy should be provided to the affected individual. Notice is:

> inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus

[48] http://hudoc.echr.coe.int/eng?i=001-57510.

> able to challenge their justification retrospectively.

Szabó, App. No. 37138/14, Eur. Ct. H.R., at 43. Therefore, "[a]s soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure" it should be provided to the affected persons. *Id.* at 43; *see also* C-203/15, *Tele2 Sverige AB v. Post-och telestyrelsen*, 2017 E.C.R. 970, ¶ 121 (stating authorities must "notify the persons affected... as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities" and recognizing notice as essential to "their right to a legal remedy.).

If notice is not provided, "any person who suspects that his or her communications are being or have been intercepted" must be capable of "apply[ing] to courts [for relief[], so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communication." *Zakharov*, App. No. 47143/06, Eur. Ct. H.R., at 59. *see also id.* at 75 (faulting Russian law for the failure to provide notice and where access to information about interception "is conditional on the person's ability to prove that his or her communications were intercepted").

* * *

This case marks a pivotal moment in the ongoing effort to safeguard privacy in the modern age. The decision will have broad implications for the development privacy laws worldwide. The European Court of Human Rights has stated recently, "technological advances . . . the potential interferences with email, mobile phone and Internet services as well as

those of mass surveillance attract the Convention protection of private life even more acutely" than ever before. *Szabó*, App. No. 37138/14, Eur. Ct. H.R., at 33. The Supreme Court of the United States should recognize that unilateral assertion of authority to access data abroad would offend comity, undermine treaty obligations, and disrupt international efforts to seek consensus on a common problem

The Court's presumption against the extraterritorial application of U.S. law is sound. The Court should also respect the jurisprudence of the European Court of Human Rights and the European Court of Justice in a matter that concerns police searches in Ireland, a member of the Council of Europe and the European Union.

CONCLUSION

For the foregoing reasons, *amici* respectfully ask this Court to affirm the decision of the U.S. Court of Appeals for the Second Circuit.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
ELENI KYRIAKIDES
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

January 18, 2018